Office/Contact: Division of Technology and Security
Source: SDBOR Policies 7.1 and 7.4
Link: https://public.powerdms.com/SDRegents/documents/1727287; https://public.powerdms.com/SDRegents/documents/1727297

SOUTH DAKOTA STATE UNIVERSITY
Policy and Procedure Manual

SUBJECT: Password Requirements
NUMBER: 7:6

---

1. Purpose

   This policy establishes the University's standard for creation of strong passwords, the protection of those passwords, and the frequency of change. All individual users are responsible for safeguarding their system access username and password credentials and must comply with the password standards identified in this policy.

2. Policy

   a. All passwords shall automatically expire and will be changed on a regular basis by the account owner, as defined and in compliance with the University Password Protection Standards document maintained by Information Technology & Security.

   b. All passwords shall be strong passwords, as defined in the University Password Protection Standards document maintained by Information Technology & Security.

   c. Passwords should not be shared with anyone. Sharing or allowing another individual to use an account password is a violation of SDBOR Policy 7.1 and University Policy 7:5, (Acceptable Use Policy) and other applicable policies. All passwords are to be treated as sensitive, confidential information.

      i. If a password must be shared to address a technical issue, it shall be changed immediately after the issue is resolved.

      ii. If a password must be shared with an external vendor, written approval must be granted by the Office of Information Technology & Security before sharing the password and the password must be immediately changed when the work is completed.

   d. Passwords must not be written down, stored, or transmitted in a form that is consumable or readable by an unauthorized observer.

   e. Accounts or passwords compromised or suspected of being compromised shall be immediately reported to the Information Technology Security Operations Center.

f. Passwords that are compromised or suspected of being compromised must be changed immediately.

g. The University, including its colleges and departments, will never request user account credentials by phone, email, or text message. Any such requests shall be reported to the Information Technology Security Operations Center immediately.

h. Exceptions to this Policy or Standards require the written approval of the VP for Technology & Security.

3. Responsible Administrator

   The VP for Technology & Security, or designee, is responsible for the annual and ad hoc review of this policy and its procedures. The University President is responsible for formal policy approval.

SOURCE: Approved by President 11/17/2015. Revised; Interim Revisions Approved by President on 11/6/2023. Revised; Approved by President on 02/14/2024.